ABSTRACT OF THE DISCLOSURE:

A digital signature system comprises a center computer and a first and second terminal devices which can communicate with each other. The center computer generates and outputs a signing-key for a signer and a verification-key for a verifier. The first terminal device accepts the signing-key, generates a digital signature for a digital data to be signed using the signing-key, and outputs the digital signature. The second terminal device accepts the verification-key, the signer's identification code (e.g. the unique code of the signer), an identification code of the digital data and the digital signature, and verifies the validity of the digital signature using the verification-key, the identification code of the digital data and the signer's identification code.